# 一种支持撤销的位置分层属性加密研究 *

沈学利，崔海韵，陈鑫彤

(辽宁工程技术大学 电子与信息工程学院, 辽宁 葫芦岛 125105)

**摘　要：** 基于属性加密的位置分层访问方案允许用户依据自身的情况灵活设置自己的位置访问信息，不仅解决了社交网络中位置共享问题，还在算法上进行改进使解密效率得以提升。但在系统运行过程中，存在用户有更正自己属性信息的需求或运行过程中部分私钥遭泄露的可能，因此支持撤销对于系统安全非常必要。基于此提出了一种支持撤销的位置分层属性加密方案，将部分解密运算外包给解密服务器，并结合了双因子身份认证的方法。该方案在减少用户的计算代价的同时，提高了算法的安全性。

**关键词：** 属性加密；撤销；位置分层；解密外包；双因子身份认证

**中图分类号：** TP309.7　　doi: 10.19734/j.issn.1001-3695.2018.06.0477

# Research on encryption of location hierarchical attributes supporting revocation

Shen Xueli, Cui Haiyun, Chen Xintong

(*School of Electronics & Information Engineering Liaoning Technical University*, *Huludao Liaoning* 125105, *China*)

**Abstract:** The location-based hierarchical access scheme based on attribute encryption allows users to flexibly set their own location access information according to their own situation. Not only solving the problem of location sharing in social networks, but also improving the algorithm to improve the decryption efficiency. However, during the operation of the system, there is a possibility that the user has corrected his own attribute information or the private key may be leaked during the operation, supporting the withdrawal is very necessary for system security. Based on this, a location hierarchical attribute encryption scheme supporting undo is proposed, which outsources part of the decryption operation to the decryption server and combines the method of two-factor identity authentication. This solution reduces the user's computational cost and improves the security of the algorithm.

**Key words:** attribute encryption; revocation; hierarchical access control; outsourced decryption; two-factor authentication



## 0　引言

云存储是一种基于云计算建立起来的网络存储技术，随着互联网的飞速发展，云存储也成为信息技术领域研究的热点。近年来各种定位服务逐渐增多，在分布式开放的网络环境下，社交网络中的用户可以享受多样性的定位服务，比如车辆的导航服务，酒店查询服务等。但用户在享受服务多功能性的同时，也注意到了社交软件中存在的安全性问题。为了提高自身定位信息的安全性，相关的位置信息保护方法也得到重视。目前保护个人位置信息的常用方法大致可以分成两类：空间位置隐藏技术[1]和虚假定位技术[2]，这两种方法都是通过模糊用户的位置信息、制造虚假信息来混淆攻击者，以达到保护信息的目的，但是都不能允许用户进行细粒度的访问控制，也不能根据用户的特定需求提供最简洁的位置信息，同时也很容易导致信息被泄露。

针对上述问题，Lin 等人[6]在传统的基于属性加密算法[3]的基础上提出了基于属性加密的新算法，并借鉴文献[4,5]中的线性秘密共享方案设计了一种位置分层访问控制方案，该方案以属性加密和对称加密混合的方式加密用户位置信息，让用户可以根据自己的需求设定位置信息访问策略。但是用户权限会随着用户修改属性发生变化，Lin 等人所提的方案中，并不能实现属性的及时撤销。Pirretti 等人[7]于 2006 年又提出了密文策略的属性撤销方案，其思想是中央机构周期性更新被设定有效期的属性的版本，撤销指定属性即可达到用户撤销的目的。Hur 等人[8]在 2011 年提出一种支持撤销的属性基加密方案，可以在外包的环境下实现细粒度访问控制，但不能抵抗用户合谋攻击。Zhao 等人[9]提出了一个两方计算的可撤销 CP_ABE 方案，需要将属性中心拆分为属性权威和中央控制。

在分布式开放的网络环境下，对使用者的身份认证是确保安全的基础和关键。双因子身份认证技术弥补了传统密码认证

---

**收稿日期：** 2018-06-21；**修回日期：** 2018-08-28　　**基金项目：** 国家自然科学基金资助项目（61602227）

**作者简介：** 沈学利（1969-），男，江苏连云港人，教授，硕士，主要研究方向为网络安全，计算机网络（523419858@qq.com）；崔海韵（1994-），女，辽宁鞍山人，硕士研究生，主要研究方向为网络安全；陈鑫彤（1995-），女，辽宁辽阳人，硕士研究生，主要研究方向为网络安全.

方法中的存在的某些弊端。也为用户登录提供了安全性保障。1999 年，Yang 等人[10]推出了第一个基于智能卡的密码认证方案，它并没有设置一个敏感信息存储表，这是该方案相较于传统方案的一个关键优势。为了保护与静态用户相关的 ID 信息，Das 等人[11]提出了一种可行方法，即采用"动态 ID 技术"，解决了信息遭受攻击的问题。2015 年，Wang 等人通过对两个最重要的匿名双因子方案[12, 13]进行密码分析后提出了一个分布式系统中的双因子身份验证方案[14]，经分析与验证，该方案安全性更强。

为了解决上述问题，参考已有的支持撤销的 CP_ABE 解密方案[15]，本文提出了一种可撤销的位置分层属性加密方案，本方案支持细粒度的属性撤销和用户撤销，提高了系统的安全性。为了减少用户的计算负担将解密时复杂的计算外包给代理商，使系统更为灵活。又结合已有的匿名双因子认证机制[14]，进一步保护用户的隐私与数据安全。

## 1　相关知识

### 1.1　双线性映射

$G_1$ 和 $G_2$ 是乘法循环群,且阶为素数 p。满足下列属性:

1)双线性

对于 $\forall u,v \in G_1, a,b \in Z_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$；

2)非退化性

$\exists u,v \in G_1$ 使得 $e(u,v)\neq 1$；

3) 可计算性

对于 $\forall u,v \in G_1$,可以有效计算出 $e(u,v)$。

### 1.2　线性秘密共享

定义参与者集合为 P，如果 P 上的某一个秘密共享方案满足如下两个条件，则为线性的。

a）每个参与者的秘密值表示 $Z_p$ 上的一个向量。

b）$M$ 是一个 $l\times h$ 的矩阵，映射函数将矩阵 M 的每一行对应一个属性值，第 i 行对应第 i 个属性。随机选择列向量 $v=(s,r_2,\dots,r_n)$，其中 $s\in Z_p$，s 表示秘密值,r 为 $Z_p$ 中的一组随机数。令 $\lambda_i = M_i \cdot v, i=1,2,\dots,l$，$\lambda_i$ 是秘密 s 的第 i 个值，$\lambda_i$ 属于参与者 $\rho(i)$。

每个线性秘密共享方案都满足线性重组的性质：假设$\mathcal{B}$是访问结构 A 的一个线性秘密共享方案，S 是 A 中的任意授权集合，定义 $I=\{i:\rho(i)\in S\}$,如果 $\{\lambda_i\}$ 是秘密 S 的有效值，就一定存在常数集合 $\{\omega_i \in Z_p\}_{i\in I}$，使得 $\sum_{i\in I}\omega_i\lambda_i = s$.

### 1.3　Diffie-Hellman DBDH 假设

挑战者基于系统的安全参数，随机选取 $a,b,c,t\in Z_p$。定义双线性映射 $e:G_1\times G_1 \to G_2$，g 为 $G_1$ 的生成元，素数 P 是群组 $G_1$，$G_2$ 的阶。

敌手优势为 $\Pr[b=b']-1/2$，且无法以不可忽略的优势从中 $(g^a,g^b,g^c,e(g,g)^t)$ 判定出 $(g^a,g^b,g^c,e(g,g)^{abc})$.

### 1.4　双因子身份认证

双因子身份认证分以下两个阶段：注册阶段，验证阶段。其中 S 为服务器，x 为 S 的私钥，哈希函数 $H(\cdot):\{0,1\}^* \to \{0,1\}^k$，P 为椭圆曲线 $E_p$ 的基点，用户注册时间为 T。

1)注册阶段

用户 $U_i$ 选择自己的身份 $ID_i$ 并且自由设置密码 $PW_i$。再选择一组随机数 $n_i$。随后用户通过安全信道将信息发送至服务器 S。则服务器从用户 $U_i$ 处收到请求

$$\{ID_i, H, (PW_i \| n_i)\}$$

服务器 S 选择随机数 $m_i$ 并计算安全的参数

$$Q = H(PW_i \| n_i) \oplus H(ID_i \| x \| T)$$

继续发送给用户：$S \Rightarrow U_i : Q$

用户将私钥 $n_i$，安全参数 Q 存入智能卡中。

2)验证阶段

当用户 $U_i$ 想要访问服务器 S 时，用户将插入智能卡，并输入自己的身份 $ID_i$，密码 $PW_i$。智能卡进行预先计算

$$Q^* = H(PW_i \| n_i) \oplus H(ID_i \| x \| T)$$
$$e = a_1 \times P, c = a_1 \times P_s$$

存储并保留信息 $\{Q^*, e, c, a_1\}$

用户计算 $H(ID_i \| x \| T) = H(PW_i \| b) + Q$，选择随机数 $a_2$，计算 $M_1 = (ID_i \| H(ID_i \| x \| T) \oplus a_2)) \oplus H(c)$，并将信息返回给服务器 S。

S 选择随机数 $a_s$,进行以下计算:

$$H(e\times x) \oplus (ID_i \| H(ID_i \| x \| T) \oplus a_2)) \oplus H(c) = H(e\times x) + M_1$$
$$M_2 = H(H(ID_i \| x \| T) \| a_2 \| e)$$
$$SK = H(M_2 \| e \| a_s \times a_1 \times P)$$
$$M_3 = H(SK \| H(ID_i \| x) \| M_2 \| a_2 \| e)$$
$$S \to U_i : \{M_2, M_3\}$$

收到 S 的回复后，用户计算:

$$SK = H(M_2 \| e \| a_s \times a_1 \times P)$$
$$M_3^* = H(SK \| H(ID_i \| x) \| M_2 \| a_2 \| e)$$

并进一步判断，

若 $M_3^* = M_3$，则 $U_i \to S : \{NULL\}$

若 $M_3^* \neq M_3$，用户计算 $M_4 = M_3$

$U_i \to S : \{M_4\}$,即 S 收到 M4 后,执行以下操作

若 $M_4^* = H(SK \| H(ID_i \| x) \| M_2 \| a_2 \| e) = M_4$，那么 S 准许 $U_i$ 的请求。反之，则用户被拒绝。

### 1.5　安全模型

本方案通过挑战者和敌手之间的对弈游戏来描述支持撤销的位置分层加密方案的安全模型。具体过程如下：

Setup()　挑战者运行算法 Setup(),输入公共参数 $PPA$，并将输出的公开密钥PK和属性公开密钥 $PK_{att}$ 以及公共参数发送给敌手。

Phase 1　挑战者提交一个集合 $D=\{I_{key}\}$ 并设置整数 k=0，敌手可以向挑战者重复进行如下询问：

转换密钥询问：挑战者选择 k=k+1,随后运行 $I_{key}$ 外包密钥

算法，挑战者返回相应的转换密钥 TK。

属性密钥查询：敌手提交一个对应于 $I_{key}$ 的访问策略进行查询，再将生成的相应属性密钥 SK 传送给攻击者。

Challenge　敌手提交两个长度相等的信息 $M_0, M_1$ 和 $I^*$，其中 $I_{key}$ 对应的解密密钥不能满足 $I^*$ 的访问策略。挑战者随机选择选择 $b \in \{0,1\}$，并以 $I^*$ 加密 $M_b$，将加密后的 $CT^*$ 发送给敌手。

Phase 2　类似 phase1，但敌手不能直接查询可以解密 $M_b$ 的密钥对 $CT^*$ 进行解密。

Guess　敌手输出对 $b$ 的猜测值 $b'$，若 $b' = b$，则敌手获得成功。该实验过程中，敌手的优势为

$$\Pr[b = b'] - 1/2 = 0。$$

定义 1　如果任何多项式时间敌手在实验过程中都无法以不可忽略的优势赢得选择明文攻击下的安全游戏，则该方案是安全的。

## 2　方案设计

本文在基于属性加密位置分层访问策略[6]的基础上，引入解密外包，结合了双因子身份验证的方法，提出了一种支持撤销的 CP_ABE 加密方案。

### 2.1　用户注册及系统初始化

a）服务器 S 选取一个椭圆曲线 $E_p$，G 为阶为 n 的基点，$P_s = x \times P$ 为系统的公钥。用户输入自己的 $ID_i$ 和 $PW_i$。

S 从 $U_i$ 处收到用户的请求并随机选择参数 $m_i$，计算 $Q = H(PW_i \| n_i) \oplus H(ID_i \| x \| T)$。将安全参数发送给用户，用户保存私钥 $n_i$，注册完毕。

b）Setup($1^\lambda$):定义一个哈希函数 $H:\{0,1\}^* \to G$ 和有效的双线性映射 $e: G_1 \times G_1 \to G_2$，$G_1$ 和 $G_2$ 两个阶为素数 p 的乘法循环群，g 是 $G_1$ 的生成元。A 表示主属性集合 $A = \{h_1, h_2, \cdots, h_u\}$，其中 $h_1, h_2, \cdots, h_u \in G_1$，$A'$ 为次要属性集合 $A' = \{n_1, n_2, \cdots, n_u\}$，$n_1, n_2, \cdots, n_u \in Z_p$ 为系统中每一个属性设置主属性编号 $V_{att}$，次属性编号 $V_{att'}$ .

系统进行初始化，以安全参数 $\lambda$ 作为输入，AA 随机选择 $\alpha, \beta, n_0 \in Z_p$，计算系统公钥 $PK =< g, e(g,g)^\alpha, g^\beta, g^{n_0}, h_1, h_2, \cdots, h_u,$ 和公开属性密钥 $g^{\alpha n_1/n_0}, g^{\alpha n_2/n_0}, \cdots, g^{g^{\alpha n_u/n_0}}, H >$ $PK_{att} = g^{V_{att}}$，$PK_{att'} = g^{V_{att'}}$ 再设置主密钥 $MSK=\{\alpha, \beta, n_0, \{V_{att}\}_{att \in S}, \{V_{att'}\}_{att' \in S'}\}$,AA 秘密保留 MSK。最后将 PK 和 $PK_{att}$、$PK_{att'}$ 发送给代理商。

### 2.2　加密算法

$Encrypt(PK, PK_{att}, k_1, (M, \rho))$:数据拥有者依据用户位置信息的分层策略使用对称加密算法（以 E 表示）生成三组对称密钥 k1,k2,k3，直接将对称密钥 k1,k2,k3 定义为密文。随机加密位置信息 m1,m2,m3,得到加密密文

$$E_{k_1}(m_1), E_{k_2}(m_2), E_{k_3}(m_3)$$

输出密文 $CM =< E_{k_1}(m_1), E_{k_2}(m_2), E_{k_3}(m_3) >$ .

数据拥有者再进一步对对称密钥 k1,k2,k3 进行加密，根据文献[5]提到的方法构造一个基于属性的访问策略 $(M, \rho)$，其中的 LSSS 矩阵用以表示主策略 P1，M 表示一个 l 行 h 列的矩阵，$\rho$ 是映射函数。随机产生列矢量 $\vec{V} = (s, v_2, \ldots, v_h) \in Z_p$，计算 $\lambda = \vec{v} \cdot \mathrm{M_i}, i = 1, 2, \ldots, l$，其中 s 表示待共享的秘密。随机从 $Z_p$ 中选择 $r_1, r_2, \cdots, r_i$，然后计算

$$\tilde{C}_1 = k_1 e(g,g)^{\alpha s} \qquad C' = g^s$$
$$\left(C_1 = g^{\beta\lambda_1} g^{V_{att}} H(\rho(i))^{-r_1}, \ D_1 = g^{r_1}, (M, \rho)\right), \ \ldots,$$
$$(C_l = g^{\beta\lambda_l} H(\rho(l))^{-r_l}, \ D_l = g^{r_1}, (M, \rho))$$

以上为第一阶段加密。

$Encrypt(PK, PK_{att'}, k_2, k_3, (M, \rho))$:在加密 k2,k3 的过程中,以系统公钥 PK 中 $g^{n_0}$ 和 $g^{\alpha n_1/n_0}, g^{\alpha n_2/n_0}, \cdots, g^{g^{\alpha n_u/n_0}}$ 计算:

$$\tilde{C}_2 = k_2 e(g^{n_0 s}, g^{\alpha n_3/n_0}) = k_2 e(g,g)^{\alpha s n_3}$$
$$\tilde{C}_3 = k_3 e(g^{n_0 s}, g^{\alpha n_3/n_0} g^{\alpha n_4/n_0}) = k_3 e(g,g)^{\alpha s(n_3+n_4)}$$

输出对称密钥密文

$$\mathrm{CT} =< \tilde{C}_1, \tilde{C}_2, \tilde{C}_3, \ C', (C_i, D_i)_{\{i \in l\}} >$$

第二阶段加密结束。

### 2.3　身份认证及私钥生成

a）用户完成登录后，智能卡保留预先计算的信息 $\{Q^*, e, c, a_1\}$，其中 $Q^* = H(PW_i \| n_i) \oplus H(ID_i \| x \| T)$。

用户选择随机数 $a_2$，计算 $M_1 = (ID_i \| H(ID_i \| x \| T) \oplus a_2)) \oplus H(c)$ 后，将 M1 发送给 S。

服务器进行如下计算：

$$H(ID_i \| x \| T) \oplus a_2) \oplus H(c) \| ID_i = H(e \times x) + M_1$$
$$M_2 = H(H(ID_i \| x \| T) \| a_2 \| e)$$

随后选择随机数 $a_s$，将计算所得的 $SK = H(M_2 \| e \| a_s \times a_1 \times P)$, $M_3 = H(SK \| H(ID_i \| x) \| M_2 \| a_2 \| e)$ 发送至用户处。

用户判断 $M_3^*$ 与 $M_3$ 是否相等,若不相等,那么用户被拒绝;若相等，用户则继续计算 M4，最后由服务器执行计算 $M_4^* = H(SK \| H(ID_i \| x) \| M_2 \| a_2 \| e)$;若 $M_4^*$ 不等于 $M_4$，则用户身份验证失败；若 $M_4^* = M_4$，用户身份验证成功。可继续执行私钥算法。

b）$KeyGen(MSK, u)$:用户输入私钥 MSK，AA 运行密钥产生算法，随机选择唯一的 $t \in Z_p$，结合主属性集合和次要属性集为合法授权用户 $u$ 得到转换密钥

$$\mathrm{TK} =< K_s = g^\alpha \cdot g^{\beta t}, K_{s'} = g^{\alpha/t} \cdot g^{\beta t}, \ L = g^t,$$
$$\{\mathrm{K_{att}} = (\mathrm{g}^{\mathrm{V_{att}}} \mathrm{H(x)})^t\}_{\forall \mathrm{att} \in \mathrm{S}}, \{K_{x'} = (g^{V_{att'}} H(x))^t\}_{\forall att' \in S'} >$$

转换密钥 TK 发送至代理商，用户私钥 $SK = \{t\}$ 通过安全信道发给用户。

### 2.4 解密算法

$Decrypt(CT',SK)$ 接收到用户的请求后，代理商输入对应的转换密钥 TK,密文 CT，运行转换算法判断用户属性是否满足主访问策略，若满足，则可在多项式时间内计算得一组常数 $\{w_i \in Z_p\}_{i\in I}$，令 $\mathrm{I}\in\{1,2,\ldots,\mathrm{l}\}$，$\mathrm{I}=\{\mathrm{i}:\rho(\mathrm{i})\in \mathrm{S}\}$，且 $\sum_{i\in I} w_i\lambda_i = s$ 成立。计算部分解密密文

$$\begin{aligned}\mathrm{CT}_1^{'} &= e(C^{'},K_s)/\prod_{i\in I}(e(C_i,L)\cdot e(D_i,k_{\rho(i)}))^{w_i}\\ &= e(g,g)^{\alpha s}\cdot e(g,g)^{\beta st}/(\prod_{i\in I} e(g,g)^{t\beta\lambda_i w_i})\\ &= e(g,g)^{\alpha s}\end{aligned}$$

继续判断用户属性是否匹配次要访问策略，利用上阶段计算结果得

$$\begin{aligned}& e(C^{'},K_s)/\prod_{i\in I}(e(C_i,L)\cdot e(D_i,k_{\rho(i)}))^{w_i}\\ &= e(C^{'},K_s)/e(g,g)^{\beta st}\\ &= e(g,g)^{\alpha s/t}\end{aligned}$$

同解密第一阶段,计算其余的部分解密密文

$$CT_2^{'} = e(g,g)^{\alpha s n_3} = (e(g,g)^{\alpha s/t})^{n_3 t},$$

$$CT_3^{'} = e(g,g)^{\alpha s(n_3+n_4)} = (e(g,g)^{\alpha s/t})^{n_3 t+n_4 t}$$

将部分解密密文 $\mathrm{CT}_1^{'}$，$\mathrm{CT}_2^{'}$，$\mathrm{CT}_3^{'}$ 发送给用户 。用户计算

$$\mathrm{k}_1 = \tilde{\mathrm{C}}_1/e(g,g)^{\alpha s},\mathrm{k}_2 = \tilde{\mathrm{C}}_2/e(g,g)^{\alpha s n_3},$$

$$\mathrm{k}_3 = \tilde{\mathrm{C}}_3/e(g,g)^{\alpha s(n_3+n_4)}$$

最终通过对称密钥 $k_1,k_2,k_3$ 得到解密后的明文信息：

$$m_1 = D_{k_1}(E_{k_1}(m_1)),\ \ m_2 = D_{k_2}(E_{k_2}(m_2)),\ \ m_3 = D_{k_3}(E_{k_3}(m_3))$$

### 2.5 属性撤销

该阶段撤销方案分为用户撤销和属性撤销两部分。

AA 撤销指定用户时，该用户离开系统后无法解密数据服务器里的任何信息，用户 u 的访问权限被撤销。AA 设置一个撤销列表，令 $RT = RT \cup \{u\} = \perp$。位于列表上的用户将被代理商拒绝返回部分解密密文，即实现用户撤销。

撤销用户的主要属性 $att_1$ 时，输入主密钥 MSK 和属性密钥 $PK_{att_1}$，为该属性随机选择产生新的属性编号 $\overline{V}_{att}$，属性权威计算并输出更新后的公开属性密钥 $PK_{att_1}$ 并向数据拥有者发布公告，公开属性公钥已更新为 $\{g^{\overline{V}_{att}}\}$.

AA 为拥有该属性的用户产生转换密钥的更新密钥 $UUK = g^{(\overline{V}_{att_1}-V_{att_1})}$，并通过安全信道将更新密钥发送给代理商，部分用户仍拥有已撤销属性，代理商为其更新后的转换密钥为

$$\begin{aligned}TK^* =&< K_s^* = g^{\alpha}\cdot g^{\beta t}, K^*_{s^{'}} = g^{\alpha/t}\cdot g^{\beta t},\ L^* = g^t,\\ &\{\mathrm{K_{att}} = (\mathrm{g^{V_{att}}H(x)})^{\mathrm{t}}\}_{\forall\mathrm{att}\in\mathrm{S}}, \{K^*_{x^{'}} = (g^{V_{att^{'}}}H(x))^t\}_{\forall att^{'}\in S^{'}},\\ &K_{att_1} = K_{att}\cdot UUK >\end{aligned}$$

为了避免新用户满足访问策略时无法访问之前的密文，所有访问策略里包含已撤销属性 $att_1$ 的关联密文需要进行更新。AA 产生密文更新密钥 $CUK = D_i^{-(\overline{V}_{att_1}-V_{att_1})}$ 并发送给代理商，代理商将所有包含属性 $att_1$ 的密文进行升级，更新后的密文为

$$\tilde{C}_1^* = k_1 e(g,g)^{\alpha s} \qquad C^{'*} = g^s$$

$$(C_1^* = g^{\beta\lambda_1} g^{V_{att}} H(\rho(i))^{-r_1}\ ,\ D_1^* = g^{r_1},(M,\rho)),\ \ldots,$$

$$(C_l^* = g^{\beta\lambda_l} H(\rho(l))^{-r_l},\ D_l^* = g^{r_1},(M,\rho))$$

$$\tilde{C}_2^* = \mathrm{k}_2 e(g^{n_0 s}, g^{\alpha n_3/n_0}) = \mathrm{k}_2 e(g,g)^{\alpha s n_3}$$

$$\tilde{C}_3^* = k_3 e(g^{n_0 s}, g^{\alpha n_3/n_0} g^{\alpha n_4/n_0}) = k_3 e(g,g)^{\alpha s(n_3+n_4)}$$

$$\mathrm{CT} =< \tilde{C}^*_1, \tilde{C}^*_2, \tilde{C}^*_3,\ \mathrm{C}^{'*}, (C_i^*, D_i^*)_{\{i\in I\}} >$$

撤销次要属性 $att_2$ 时，与上述撤销主属性过程类似，代理商通过属性权威产生的新的转换密钥 $UUK = g^{(\overline{V}_{att_2}-V_{att_2})}$ 和密文密钥 $CUK = D_i^{-(\overline{V}_{att_2}-V_{att_2})}$ 对 TK 和密文 CT 进行更新，得到

$$\begin{aligned}TK^* =&< K_s^* = g^{\alpha}\cdot g^{\beta t}, K^*_{s^{'}} = g^{\alpha/t}\cdot g^{\beta t},\ L^* = g^t,\\ &\{\mathrm{K_{att}} = (\mathrm{g^{V_{att}}H(x)})^{\mathrm{t}}\}_{\forall\mathrm{att}\in\mathrm{S}}, \{K^*_{x^{'}} = (g^{V_{att^{'}}}H(x))^t\}_{\forall att^{'}\in S^{'}},\\ &K_{att_2} = K_{att}\cdot UUK >\end{aligned}$$

$$\mathrm{CT} =< \tilde{C}^*_1, \tilde{C}^*_2, \tilde{C}^*_3,\ \mathrm{C}^{'*}, (C_i^*, D_i^*)_{\{i\in I\}} >$$

## 3 安全性分析

### 3.1 选择明文攻击

Setup 挑战者初始化程序，输出公共参数 PPA，公开密钥 PK 和属性公开密钥 $PK_{att}$.

Phase 1

a)转换密钥查询。敌手可以重复询问已经掌握的主要属性信息 $l_1,l_2,\cdots,l_k$，挑战者通过运行外包的密钥算法 $I_{key}$，获得转换密钥 TK 和私钥 SK。根据 DBDH 假设，敌手的优势为 $\Pr[b=b^{'}]-1/2=0$，此时敌手无法获得与明文对应的私钥 SK。

随后输出

$\mathrm{TK} =< K_s = g^{\alpha}\cdot g^{\beta t},\ L = g^t, \{\mathrm{K_{att}} = (\mathrm{g^{V_{att}}H(x)})^{\mathrm{t}}\}_{\forall\mathrm{att}\in\mathrm{S}} >$ 再将转换密钥 TK 发送给敌手。

b)用户私钥查询。转换密钥 TK 对应私钥 SK，由于 TK 与对应的主属性集合均不能与密文 $M_b$ 的访问策略匹配，敌手试图组合不同的转换密钥 TK 的访问策略来攻击位置信息 $m_1$ 的访问策略。但本文中所有属性的访问策略都有随机参数 t，根据转换算法，计算

$$e(C^{'},K_s)/\prod_{i\in I}(e(C_i,L)\cdot e(D_i,k_{\rho(i)}))^{w_i}$$

输入用户 1 和 2 的参数 $t_1,t_2$，两者试图联合并扩张自己属性集进行攻击，则计算出结果

$$e(g,g)^{\alpha s/t}/e(g^{r_i\cdot w_i},(g^{V_{att}}\cdot H(x))^{(\frac{t_1-t_2}{t_1\cdot t_2}\cdot\beta)})$$

根据 DBDH 假设，此时敌手无法计算出

$$e(g^{r_i \cdot w_i},(g^{V_{att}} \cdot H(x))^{(\frac{t_1-t_2}{t_1 \cdot t_2} \cdot \beta)})$$

敌手优势可以忽略，将 SK 发送给敌手。

Challenge　敌手提交两个明文信息 $M_0$ 和 $M_1$，另外生成 $I^*$，并且 $I_{key}$ 的所有解密密钥生成私钥与 $I^*$ 对应的访问策略不匹配，即是无法解密。挑战者随机选择 $b \in \{0,1\}$，对明文 $M_b$ 进行加密，并将密文 $CT^*$ 发送给敌手。

Phase 2　重复 phase 1 的查询步骤。

Guess　将敌手对 $b$ 的猜测 $b'$ 输出，对密文 $CT^*$ 进一步作出判断，确认其是否为 $M_0$ 和 $M_1$ 加密后的密文，即 $b$ 是否与 $b'$ 的值相等，若 $b = b'$ ,则敌手成功。

上述过程中，敌手的优势为 $\Pr[b=b']-1/2$ .

### 3.2　数据保密性

数据的保密性定义为只有合法用户和数据拥有者可以解密获得明文消息。非法用户，已撤销的用户都无法访问数据。 在本文方案中，加密的第二阶段的安全性依赖于 Elgamal 算法中离散对数分解的 NPC 问题。假设未授权用户已满足第一阶段访问策略 $(M,\rho)$，解密获得对称密钥 $k_1 = e(g,g)^{\alpha s}$，该用户想继续攻击并得到密钥 $k_2 = \tilde{C}_2 / e(g,g)^{\alpha s n_3}, k_3 = \tilde{C}_3 / e(g,g)^{\alpha s(n_3+n_4)}$，必须能够得到随机数 $n_3,n_4$。然而从系统公钥 PK 的 $g^{\alpha n_1/n_0}, g^{\alpha n_2/n_0}, \cdots, g^{\alpha n_u/n_0}$ 中计算出 $n_3$ 和 $n_4$ 的值是难以实现的，此种计算问题属于离散对数分解的 NPC 难题，从而可以验证数据的保密性。

### 3.3　抵抗合谋攻击

在解密的第一阶段，用户必须首先得到 $e(g,g)^{\alpha s}$，才能解出对称加密密钥 $k_1$。 通常的情况下，若两个用户都不能满足主要策略，则用户不能从 $\prod_{i \in I}(e(C_i,L) \cdot e(D_i,k_{\rho(i)}))^{w_i}$ 中恢复出秘密值 S。但也存在这两个用户会满足主要属性策略的某一部分的情况，此时可以通过交换主属性参数达到扩展权限的目的。由此将随机数 t 引入转换密钥 TK，本文中所有的$K_x$都含有一个参数 t,合谋用户无法通过他们掌握的私钥组合进行解密。解密第二阶段，用户的目的是想要获取密钥 $k_2$，$k_3$，此时用户若已经从第一阶段解密过程中获得 $e(g,g)^{\alpha s}$，也需要 $n_3$，$n_3+n_4$ 配合解密。本文的系统并没有直接释放用户希望的参数 $n_1,n_2,\ldots,n_u$，而是选择释放次要属性参数，则用户不能解密。继续讨论，当两个用户都无法满足次要属性策略时不能访问存在于私钥中的 $n_3$，$n_3+n_4$，无法解密。与部分次要属性策略匹配的用户，可以交换自身的参数 $n_1,n_2,\ldots,n_u$ 进行配合攻击，和第一阶段采用同样的思想，同样选择随机数 t，此时合谋用户也不能用组合私钥参数的方式来实现解密。经验证，本文的方案是可以抵抗合谋攻击的。

### 3.4　前向安全和后向安全

前向安全：被撤销属性的用户无法解密更新后的密文访问关联该属性的密文，即使他持有该属性。

后向安全：新加入的用户在 AA 更新重加密密文仍可以解密之前的密文。

以撤销次要属性 $att'$ 为例，当发生属性撤销时,AA 便会为被撤销的属性 $att'$ 产生一个新的属性编号 $V_{att'}$，并为未撤销该属性的用户升级密钥 TK，而撤销该属性的用户不能进行密钥升级，同时为相关密文进行升级。若被撤销属性 $att'$ 的用户试图使用自己之前的密钥去解密更新后的密文，根据数据解密的相关算法，最终解密结果为 $\tilde{C}_2 = k_2 \cdot e(g,g)^{\alpha s n_3 (v_{att'} - v_{att})}$，而敌手不能获得 $\alpha, s, n_3, v_{att'} - v_{att}$，所以无法解密获得 $k_2$。对于新加入的用户，他们的私钥是由更新后的属性密钥 CUK 生成。AA 将更新的属性密钥发送给代理商，代理商负责升级相关密文，所以新用户可以解密之前的密文，从而确保了方案的后向安全。

## 4　方案分析

本章主要给出本文方案与相关方案[3，5，6，8，9]在功能性、计算效率几方面进行的对比。

### 4.1　功能比较

从表 1 可以看出，文献[6]使用了分层属性加密并对算法进行了优化，但是该方案安全性和减少计算成本上有待提升。文献[8]实现了属性级的立即撤销能力，但是没有实现细粒度的访问控制。文献[9]提出的无密钥托管可撤销属性方案实现了细粒度访问控制，但需要中央控制和授权机构两方计算，不能很好地与分层属性加密相结合。本文在此基础上支持用户撤销与属性撤销，将解密过程中的大量计算外包给了代理商，减少了用户的计算负担。

表 1　方案功能对比

Table 1　Comparison of scheme functions

| 方案 | 访问结构类型 | 撤销机制 | 撤销粒度 | 支持位置分层 | 解密外包 |
|---|---|---|---|---|---|
| **文献[3]** | access tree | 无 | 无 | 否 | 否 |
| **文献[5]** | LSSS | 无 | 无 | 否 | 否 |
| **文献[6]** | LSSS | 无 | 无 | 是 | 否 |
| **文献[8]** | access tree | 可撤销 | 属性撤销 | 否 | 否 |
| **文献[9]** | LSSS | 可撤销 | 属性/用户撤销 | 否 | 是 |
| **本文方案** | LSSS | 可撤销 | 属性/用户撤销 | 是 | 是 |

### 4.2　效率分析

本文主要是针对文献[6]的安全性问题和计算量问题，提出结合支持撤销功能和解密外包的方案，与此同时要保证原方案位置分层多次加密的优势得以延续，并对加密解密效率不会造成影响。因此本文通过对两次属性加密和三次属性加密的效率进行分析，从表 2 和 3 可以看出，增加了撤销功能后不会影响原方案的加密效率，且引入的解密外包使得用户解密负担减少。对比过程中使用符号描述定义如下：p 表示双线性对运算，e 表示模指数运算，主要属性和次要属性关联的数目分别用 a，b 表示。






表 2　两次加密效率分析

Table 2　Efficiency analysis of two times attribute encrypton

| 方案 | 结构类型 | 相关属性个数 | 加密计算量 | 解密计算量 |
|---|---|---|---|---|
| 文献[3] | access tree | a+b | (4a+4b+2)e+2p | (2a+2b)e+(2a+2b+4)p |
| 文献[5] | LSSS | a+b | (6a+6b+2)e+2p | (2a+2b)e+(4a+4b+2)p |
| 文献[6] | LSSS | a+b | (3a+1)e+2p | (a+1)e+(2a+2)p |
| 本文方案 | LSSS | a+b | (3a+1)e+2p | 2e+p |

表 3　三次加密效率分析

Table 3　Efficiency analysis of three times attribute encrypton

| 方案 | 结构类型 | 相关属性个数 | 加密计算量 | 解密计算量 |
|---|---|---|---|---|
| 文献[3] | Access tree | a+b | (6a+6b+3)e+3p | (3a+3b)e+(3a+3b+6)p |
| 文献[5] | LSSS | a+b | (9a+9b+3)e+3p | (3a+3b)e+(6a+6b+3)p |
| 文献[6] | LSSS | a+b | (3a+1)e+3p | (a+2)e+(2a+2)p |
| 本文方案 | LSSS | a+b | (3a+1)e+3p | 3e+p |

## 5　结束语

本文提出的一种支持撤销的位置分层属性加密的方案，在不影响加密效率和分层功能的前提下，结合了双因子身份认证机制，增强了系统安全性，提升解密效率，减少用户计算量，方案也具有保密性和抵抗用户合谋攻击的优点。本文通过对方案进行功能对比和效率分析，结果表明所提方案具有较高的解密效率和一定的安全性。

## 参考文献：


[1] Kido H, Yanagisawa Y, Satoh T. An anonymous communication technique using dummies for location-based services [C]// Proc of International Conference, Pervasive Services. 2005: 88-97.

[2] Yiu Manlung, Christian S, Jensen, *et al.* SpaceTwist: managing the trade-offs among location privacy, query performance and query accuracy in mobile services [C]// Proc of the 24th IEEE International Conference on Data Engineering. Washington DC: IEEE Computer Society, 2008: 366-375.

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C]// Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society. 2007: 321-334.

[4] Beimel A. Secure schemes for secret sharing and key distribution [D]. Israel: Israel Institute of Technology. 1996.

[5] Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [J]. Public Key Cryptography, 2011: 53-70.

[6] Lin Xi, Han Yiliang, *et al.* Location hierarchical access control scheme based on attribute encryption [C]// Proc of the 36th Chinese Control Conference. 2017.

[7] Pirretti M, Traynor P, Mcdaniel P, *et al.* Secure attribute-based systems [C]// Proc of the 13th ACM Conference on Computer and Communications Security. 2006: 99-112.

[8] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Trans on Parallel and Distributed Systems, 2011, 22 (7): 1214-1221.

[9] 赵志远，朱智强，王建平，等. 云存储环境下无密钥托管可撤销属性基加密方案研究 [J]. 电子与信息学报, 2018, 40 (1): 1-10. (Zhao Zhiyuan, Zhu Zhiqiang. Wang Jianping, etal. Revocable attribute-based Encryption with escrow-free in cloud storage [J]. Journal of Electronics & Information Technology, 2018, 40 (1): 1-10. )

[10] Yang Wenher, Shieh Shiuhping. A Password authentication schemes with smart cards [J]. Computers & Security, 1999, 18 (8): 727-733.

[11] Das M, Saxena A, Gulati V. A dynamic ID-based remote user authentication scheme [J]. IEEE Trans on Consumer Electronics, 2004, 50 (2): 629-631.

[12] Tsai Jialun, Lo Naiwei, Wu Tzongchen. Novel anonymous authentication scheme using smart cards [J]. IEEE Trans on Ind. Inform, 2013, 9 (4): 2004-2013.

[13] Li Chunta. A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card [J]. IET Inform. Se cur, 2013, 7 (1): 3-10.

[14] Wang Ding, He Debiao, Wang Ping, *et al.* Anonymous two-factor

[15] authentication in distributed systems: certain goals are beyond attainment [J]. IEEE Trans on Dependable & Secure Computing, 2015, 12 (4): 428-442.

[16] 李勇，曾振宇，张晓菲. 支持属性撤销的外包解密方案 [J]. 清华大学学报：自然科学版, 2013, 53 (12): 1664-1669. (Li Yong, Zeng, Zhenyu, Zhang Xiaofei. Outsourced decryption scheme supporting attribute revocation [J]. J Tsinghua University: Sei&Technol, 2013, 53 (12): 1664-1669. )

[17] 池水明，陈勤，党正芹. 一种基于策略控制的可撤销属性基代理加密方案 [J]. 计算机工程与科学, 2013, 35 (9): 94-98. (Chi Shuimng, Chen Qin, Dang Zhengqin. An attribute-based encryption scheme with attribute revocation and key delegation based on policy control [J]. Computing Engineering & Science, 2013, 35 (9): 94-98. )

[18] 闫玺玺，孟慧. 支持直接撤销的密文策略属性基加密方案 [J]. 通信学报, 2016, 37 (5): 44-50. (Yan Xixi, Meng Hui. Ciphertext policy attribute based encryption scheme supporting direct revocation [J]. Journal on Communications, 2016, 37 (5): 44-50. )

[19] Huang Qinlong, Ma Zhaofeng, Yang Y, et a1. Attribute-based secure data sharing with efficient revocation in cloud computing [J]. Chinese JournalElectronics, 2015, 24 (4): 862-868.